# Clouds, services, servers

**What does it do? 600 words**

First of all, let us address what Cloud is in the first place and how it can be classified. To an

everyday non-technical user, the Cloud amusingly means files get stored in the sky

somewhere invisibly. But at a deeper level, with a better understanding, Cloud is more than

this. Your photos for smart-phone devices, digital cameras, everyday documents get stored

on services such as Google Drive, Microsoft OneDrive, DropBox, SugarSync, Apple iCloud, to

name just a few. Synchronisation across multiple devices is possible, even if they run

different operating systems.

Now let us define Cloud further -

This is how a ResearchGate publication defines this (in-citation provided)

&quot;Zhang, Qi &amp; Cheng, Lu - 2020 Journal of Internet Services and Applications. &quot;Cloud

computing has recently emerged as a new paradigm for hosting and delivering services

over the Internet. Cloud computing is attractive to business owners as it eliminates the

requirement for users to plan ahead for provisioning, and allows enterprises to start from

the small and increase resources only when there is a rise in service demand. &quot;(PDF)

Cloud Computing: State-of-the-art and Research Challenges. [online] ResearchGate.

Available at:

&lt;https://www.researchgate.net/publication/225252747\_Cloud\_Computing\_State-of-the-

art\_and\_Research\_Challenges&gt; [Accessed 9 Jul. 2020].

In my own words -

Cloud can be physical servers hosting a variety of in-house or external service provider

based resources for the end device user be it a PC, tablet, smart-phone, developers,

designers, even mechanics can use the service. It does this through the following

classifications

Public –Pooling of virtual services that provide storage and resources to everyday users –

(Storage, workloads, virtualisation) avoiding facilitation of costly storage mediums (SD

cards in phones/cameras, larger external/internal hard drives on computers and other

media such as DVD/Blu-ray optical discs)

Private – Same resources as Public Cloud, however, usually used by one

client/customer/business entity. It&#39;s not shared with others outside of the infrastructure.

This provides the possibility of on-premise Cloud in a data centre, at higher cost needing

physical servers, and management of the equipment.

Hybrid-cloud – Generally purpose-built Private/Public combination cloud services.

Examples of providers that utilise this type of service (top 5, see citations)

Top 5 Hybrid Cloud Providers:

Amazon

Microsoft

Google

Cisco

NetApp

NetApp provides on tap storage, mainly for businesses, Cisco focuses on security, networking,

and governance. Amazon provides on-demand virtualisation primarily as well as storage

(think of an appliance) Microsoft provides Storage, and is a competitor to Amazon with

it’s Azure service. In the future, I believe Cloud will be the more prominent default

storage option and also provide a virtualised desktop on the move which people will be

able to access from just about any machine and integrate storage cloud solutions into

this. Applications, files, desktop settings, preferences – basically everything is available to

the person with far less risk of things going wrong.

So in summary – Cloud is a service requiring the use of higher end computing servers either on-

premise or remotely accessed providing a convenient means of storing information that can

be accessed anywhere with an internet connection. This is what makes it all possible, faster

bandwidth. Cloud would not have thrived in the days of Napster, Lime-wire and 56K Dial up

internet when Operating systems struggled to run basic software without crashing at the

best of times.

**What is the likely impact? (300 words)**

**How will this affect you? (300 words)**

CITATIONS for in-text and research shown/provided.

Čandrlić, G., 2020. Cloud Computing - Types of Cloud. [online] Globaldots.com. Available at:

&lt;https://www.globaldots.com/blog/cloud-computing-types-of-cloud&gt; [Accessed 9 Jul. 2020].

&quot;Zhang, Qi &amp; Cheng, Lu, 2020,

&lt;https://www.researchgate.net/publication/225252747\_Cloud\_Computing\_State-of-the-

art\_and\_Research\_Challenges&gt; [Accessed 9 Jul. 2020].

Cloud, 5., 2020. 5 Real-Life Examples of Hybrid Cloud. [online] knowledgeable. Available at:

&lt;https://www.knowledgenile.com/blogs/real-life-examples-hybrid-cloud/&gt; [Accessed 9 Jul. 2020].

John Buni, C., 2020. Cloud computing could look quite different in a few years. [online] VentureBeat.

Available at: &lt;https://venturebeat.com/2019/06/02/cloud-computing-could-look-quite-different-

in-a-few-years/&gt; [Accessed 9 Jul. 2020].

# Cyber Security

**What does it do? (600 words)**

Cyber Security is the process of defending computers , servers , mobile devices , electronic systems , networks and data from malicious attacks . Cyber Security is also known as information technology security or electronic information security . Cyber security can be further divided into types of security .

Network Security - Securing a computer from network intruders .

Application security -Securing software and devices .

Operational security - The processes and decisions for handling and protecting data assets

Information security - Integrity and privacy of data .

Identity management- The process of understanding the access every individual has in an organization

Disaster recovery - How an organization deals with a cyber security breach and how it can recover .

User Education - Teaching users good security practices .

Types of cyber threats cyber security is designed to prevent are :

Cyber Crime - Targeting systems for financial gain or to cause disruption .

Cyber Attack - Information gathering usually politically motivated

Cyber Terrorism - Undermining electronic systems to cause panic and fear .

The most common types of cyber threats are:

Malware - Malicious software

SQL injection - Structured Language Query injection is where a user takes control of and steals data from a system .

Phishing - Targets users with emails that appear from a legitimate company asking for sensitive information .

Man in the Middle - Interception of communication to steal data .

Denial of service - Prevents a computer system from fulfilling a legitimate request by overwhelming networks and servers with traffic.

We’re living in a far more technologically-advanced world than we were a decade ago.Consider the fact that the iPad has only been around since 2010, and the iPhone only came out a few years before that. Average broadband speeds have increased by roughly five-fold in the last decade, making it possible for businesses and individuals to do far more online. This has facilitated the rise in cloud services, working from home and massive amounts of data being thrown back and forth .Businesses and individuals now take for granted such things as easy online document sharing, email that’s available on every device, and databases being accessible from everywhere.

The most difficult challenge in cyber security is the ever-evolving nature of security risks themselves. Traditionally, organizations and governments have focused most of their cyber security resources on perimeter security to protect only their most crucial system components and defend against known threats. Today, this approach is insufficient, as the threats advance and change more quickly than organizations can keep up with. As a result, advisory organizations promote more proactive and adaptive approaches to cyber security. Such as a shift toward continuous monitoring and real-time assessments, a data-focused approach to security as opposed to the traditional perimeter-based model.

Nobody can tell exactly what the next major cyber threat will be or where it will come from, but experts still have a good idea of the general direction that we’re heading in. AI systems are sure to become a major target for hackers when more and more companies start to use them. In response, future cybersecurity software and personnel will be forced to develop techniques to detect and counteract AI corruption attacks. Many now believe that cyberwarfare, where one nation hacks or embeds viruses in the computer systems of another, will become the frontier on which wars are fought around the world . There is good reason to believe that the number of people with the skills and motivation to hack legitimate systems will grow in the future as education improves all over the world as the potential pays off are large. Companies around the world are continuing to expose themselves to cyber risk by continuing to use vulnerable legacy technology. Usually, this is done to save money or because the business doesn’t recognize the security benefits offered by upgrading.

**What is the likely impact? (300 words)**

It’s estimated that the global cost of cybercrime for 2017 added up to around $600 Billion. With the number mounting up every year, and by 2021 experts are suggesting a figure of up to $6 Trillion per year.

54% of companies have had their network or data compromised in 2016 . The average cost of recovering from a cyber attack, is around $5 Million for a large company . 60% of small businesses who experience a major cybercrime incident go out of business shortly after.One particularly chilling statistic is that there are now over 4000 hacks every single day using ransomware alone. It’s extremely misguided for anyone to think they can't be affected.

Antivirus software is still an essential part of IT security , but it’s not enough on its own to protect from modern threats. Technical teams need many more tools, resources and solutions, and some of them are expensive. However, they’re not likely to be as expensive as the cost of recovering from a cyber attack.

It’s no longer realistic to expect an IT department to mitigate every IT security risk as many modern cyber security threats originate from social engineering, user error, exploits to web browsers, and other things that technical teams can only do so much to protect you from. Cyber security is something everyone needs to take notice of, and a huge number of incidents are caused by people ignoring IT advice such as avoiding clicking on suspicious links and maintaining secure passwords . Another good example of why cyber security isn’t merely a technology issue is how easy it is for any one in any department to cause a data breach. A breach can happen by something as simple as a distracted employee leaving an unencrypted personal device on a bus on the way to work. Everyone needs to be aware of the implications of not using cyber security .

**How will this affect you? (300 words)**

Cyber Security affects companies and big businesses so does it affect me , my parents or friends? You don't need to be a big company or big business to be targeted , breaches in personal cyber security can result in hackers claiming your financial information, work files, and even more personal information like photos and social media messages. Bad credit ratings, an inability to access your computer, or even total identify theft. If you're online you can be targeted from your emails , gaming passwords , social media and internet banking to name a few , cyber security affects Everyone in everyday life . 47.1% of Australian homes have more than five smart home devices connected, according to the Avast Smart Home Report 2019. At least 33.4% of these include at least one vulnerable connected device, this has the ability to compromise the entire home network’s security.

Currently, Australia’s cyber security workforce is short of approximately 2,300 workers, with the country needing up to 17,600 additional cyber security employees by 2026.

What can you do to increase your own security and make it harder to be targeted ?

A few simple steps can be made every time you log on :

Passwords - Big security organizations cannot protect consumers against phishing or hackers who can guess passwords like “1234.” Common sense and password hygiene can go a long way to protect you from cyber threats.

Websites- Be careful about which websites you go to , a lot of well known websites have additional security attached to make it harder to gain your information , but a dodgy website won't have the same security , some are even designed to steal your information by asking personal questions , which they can use themselves or sell/pass on to someone who will use that data for their own gain .

Anti-virus software - Subscribe to anti-virus software and keep your system up to date with automated, scheduled scans.

Phishing attacks - Be careful about opening file attachments. Phishing and spear phishing emails are ones that look real but are not. if you pay attention. For instance, if you get an email that says “past due invoice” with a PDF attachment, don’t open it unless you are 100% sure you know who sent it. If you double check, you’ll probably see it comes from an unusual email, like this one, from anny234526426@gmail.com .

REF : https://www.kaspersky.com.au/resource-center/definitions/what-is-cyber-security

https://digitalguardian.com/blog/what-cyber-security

https://www.techradar.com/news/what-is-the-future-of-cybersecurity

https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds

https://securityfirstcorp.com/why-is-cyber-security-important/

https://preyproject.com/blog/en/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them/

https://www.lifehacker.com.au/2019/06/how-cybersecurity-affects-all-aspects-of-your-life/

# Blockchain + Cryptocurrencies

**What does it do? (600 words)**

Blockchain is a public electronic ledger that is primarily built around a peer-to-peer system that is open to everyone and can show transaction history. As a transaction is made, a new block is created and has all the details of what was done but a link to the prior block to show the history of the purchase. Blockchain technology has a process called Proof or work, this is mainly in Cryptocurrency, this slows down the transaction so nothing can be doubled or corrupted in the process.

Each block has 3 main points about them: Data, Hash, Hash of the previous block. Blockchain technology cuts out the middle-man costs like transaction charges on card fees and does not have a turnaround time when transfer funds (Cryptocurrency).

Right now, with Blockchain you can, transfer cryptocurrency, transfer money, certify a supply chain i.e. Walmart, De Beers, and many other things. The state of which blockchain is in right now is unsure, people and companies around the globe are unsure on how it will go in the future and the privacy around what other people can see. Transactions take a while and there are some technologies around that do similar, if not the same as Blockchain.

Within a few years we could see Cryptocurrency and Blockchain technology take over the world with transactions like buy music or a book or ride-sharing apps, companies like Uber and Spotify could take a massive hit in the way we get around and artists making more of the money not just a small profit from how many listens/views per song.

**What is the likely impact? (300 words)**

**How will this affect you? (300 words)**

# Robots

**What does it do? (600 words)**

Robot comes from the Czech word “robota” which means “forced work or labor.” We use the word "Robot" today to mean any man-made machine that can perform work or other actions normally performed by humans, either automatically or by remote control. Robotics is the science and study of robots.

Roughly half of all the robots in the world are in Asia, 32% in Europe, and 16% in North America, 1% in Australasia and 1% in Africa. 40% of all the robots in the world are in Japan, making Japan the country with the highest number of robots.

Robots can be made from a variety of materials including metals and plastics. Most robots are composed of 3 main parts:

The Controller ‐ also known as the "brain" which is run by a computer program. Often, the program is very detailed as it gives commands for the moving parts of the robot to follow.

Mechanical parts ‐ motors, pistons, grippers, wheels, and gears that make the robot move, grab, turn, and lift. These parts are usually powered by air, water, or electricity.

Sensors ‐ to tell the robot about its surroundings. Sensors allow the robot to determine sizes, shapes, space between objects, direction, and other relations and properties of substances. Many robots can even identify the amount of pressure necessary to apply to grab an item without crushing it.

All of these parts work together to control how the robot operates.

It’s not easy to define what robots are, and it’s not easy to categorize them either. Each robot has its own unique features, and as a whole robots vary hugely in size, shape, and capabilities.

Aerospace: This is a broad category. It includes all sorts of flying robots and robots that can operate in space, such as Mars rovers.

Consumer: Consumer robots are robots you can buy and use to help you with tasks and chores. Such as a Roomba vacuum, AI-powered robot assistants, and a growing variety of robotic toys and kits.

Disaster Response: These robots perform dangerous jobs like searching for survivors in the aftermath of an emergency.

Drones: Also called unmanned aerial vehicles, drones come in different sizes and have different levels of autonomy. Such as military systems like Global Hawk, used for long-duration surveillance.

Education: This broad category is aimed at the next generation of roboticists, for use at home or in classrooms. It includes hands-on programmable sets from Lego, 3D printers with lesson plans, and even teacher robots.

Entertainment: These robots are designed to evoke an emotional response and make us laugh or feel surprise . such as the robot comedian RoboThespian.

Exoskeletons: Robotic exoskeletons can be used for physical rehabilitation and for enabling a paralyzed patient to walk again. Some have industrial or military applications, by giving the wearer added mobility, endurance, or capacity to carry heavy loads.

Humanoids: Robots which are designed to look like humans.

Industrial: Robots that mainly consist of a manipulator arm designed to perform repetitive tasks. such as systems like Amazon's warehouse robots and collaborative factory robots that can operate alongside human workers.

Medical: Medical and health-care robots include systems such as the da Vinci surgical robot and bionic prostheses, as well as robotic exoskeletons.

Military & Security: Military robots are used to replace the human need on the battlefield , either fighting or logistics .

Research: The vast majority of today’s robots are born in universities and corporate research labs. Though these robots may be able to do useful things, they’re primarily intended to help researchers .

Self-Driving Cars: Many robots can drive themselves around, and an increasing number of them can now drive you around.

Telepresence: Telepresence robots allow you to be present at a place without actually going there. You log on to a robot avatar via the internet and drive it around, seeing what it sees, and talking with people. Workers can use it to collaborate with colleagues at a distant office, and doctors can use it to check on patients.

Underwater: consisting of deep-sea submersibles, diving humanoids and bio-inspired systems .

As it is increasingly common for people to use or come into contact with robots in various situations at home and in retail stores, hotels and hospitals ,commercial and industrial robots are now in widespread use performing jobs more cheaply or with greater accuracy and reliability than humans. They are also employed for jobs which are too dirty, dangerous or dull to be suitable for humans. Robots are widely used in manufacturing, assembly and packing, transport, earth and space exploration, surgery, weaponry, laboratory research, and mass production of consumer and industrial goods.

Increasingly sophisticated machines may populate our world, but for robots to be really useful, they’ll have to become more self-sufficient. After all, it would be impossible to program a home robot to contend with every single situation it could come across , the robot would need to learn on its own and be able to adapt to the new situations it could face and that is where advances in artificial intelligence come in.

but with more advanced and sophisticated AI ,comes the questions of what ethics , morals and judgements might govern robots' behavior and if by extension robots might be able to claim any kind of social, cultural, ethical or legal rights as a construct that can think on its own.

**What is the likely impact? (300 words)**

A recent example of human replacement involves Taiwanese technology company Foxconn who, in July 2011, announced a three-year plan to replace workers with more robots. At present the company uses ten thousand robots but will increase them to a million robots over a three-year period

**How will this affect you? (300 words)**

With the changes in the number and use of robots in the industrial and civil sectors, the changes that I can see will be far more beneficial than detrimental. Some of the benefits I can see are that mass produced goods and foods stuffs should become cheaper as overheads drop in price due to a lot of the labour etc being conducted by robots .Household chores should be reduced as robots clean and maintain households freeing up a lot more time for relaxation and entertainment . Having self driving cars etc would mean you can go to parties and drink without having to worry about driving home over the limit , driving would be far safer and long trips you wouldn't arrive tired .

https://sciencetrek.org/sciencetrek/topics/robots/facts.cfm

https://www.wired.com/story/wired-guide-to-robots/

https://en.wikipedia.org/wiki/Robot

https://www.nri.com/en/knowledge/report/lst/2017/cc/papers/0201

https://robots.ieee.org/learn/types-of-robots/